



FIGURE 1

TI3C1D9814|BYE5|DIC0A802FF|DP8A|DU0|EP800|PK1|PR11|SIC0A80263|SP8A
TI3C1D9821|BY5C|DIC0A80215|DU3C|EP806|PK2|SA0000E8DA99DC|SIC0A80201
TI3C1D9834|BY4E|DIC0A802FF|DP89|DU0|EP800|PK1|PR11|SIC0A80297|SP89
TI3C1D9839|BY114|DU3A|EP1F|PK6
TI3C1D9878|BYA6|DU0|EPA6|PK1
TI3C1D9878|BYE5|DIC0A802FF|DP8A|DU0|EP800|PK1|PR11|SIC0A80297|SP8A
TI3C1D987E|BY114|DU3A|EP1F|PK6
TI3C1D988E|BY148|DIC0A80219|DP43|DU0|EP800|PK1|PR11|SIC0A80299|SP44
TI3C1D988E|BY148|DIC0A80299|DP44|DU0|EP800|PK1|PR11|SIC0A80219|SP43
TI3C1D988E|BY2E|DIC0A80219|DU0|EP806|PK1|SA009027078E8E|SIC0A80299

FIGURE 2

---Timestamp
TI-start-time in seconds (since 1970 GMT)
DU-duration of validity (for time grouping)

---Structural Fields
GB-indicator that this row is an output of grouping operation
MP-indicator that this row is a mapping or lookup row

---Key Fields (this category includes Secondary Key Fields):
CD-collection device (i.e. origin of the data)
DA-destination MAC address (as stated by ARP packet)
DD-destination domain (DNS style)
DI-destination IP number

DM-destination MAC address (true MAC address)
DN-normalised destination address
DP-destination TCP port or UDP port
EP-Ethernet protocol number
PR-IP protocol number
SA-source MAC address (as stated by ARP packet)
SD-source domain (DNS style)
SI-source IP number
SM-source MAC address (true MAC address)
SN-normalised source address
SP-source TCP port or UDP port

---Secondary Key Fields (actually, special case of Key Fields)
TF-traffic flow
AC-account category
SA-sub-account category
CC-cost centre category

---Counter fields
BY-count of bytes
PK-count of packets
HT-count of web hits

FIGURE 3